UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/590,898	08/28/2006	Kaoru Yokota	2006_1396A	4382

52349 7590 01/25/2010

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
KING, CURTIS J	

ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
01/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/590,898	YOKOTA ET AL.	
	Examiner	Art Unit	
	Curtis J. King	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 9 and 10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 9, lines 3-4 recites "each of the plurality of priority levels indicating a recording priority." No where in Applicant's disclosure does the applicant disclose priority levels indicating a recording priority, or any priority for any recording.

For purposes of advancing prosecution the examiner will interpret this limitation as the order of the articles placed in the storage device as a logical, reasonable interpretation. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 2, 4, 17, 19, 20, 21, 22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1).

1) In regard to claim 1, Ono discloses the claimed authentication system (Ono fig. 1: 10) including a plurality of wireless IC tags (Ono fig. 1: 102a & ¶0036) and an authentication apparatus (Ono fig. 1: 200) which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication (Ono ¶0038 discloses the process unit performs a desired process after the user is authenticated), the authentication apparatus (Ono fig. 1: 200) comprising: a tag verification information storage unit (Ono fig. 2: 210 discloses as an Authentication Information Holding Unit) operable to store a plurality of pieces of tag verification information (Ono ¶0038 discloses as plurality of authentication information of each IC tag) for identifying the plurality of wireless IC tags respectively (Ono ¶0038); a receiving unit (Ono fig. 2: 230 & ¶0037 discloses the personal authentication unit serves also as an authentication information receiving unit; not shown but it's inherent) operable to wirelessly receive (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from wireless IC tags (Ono fig. 1: 102a) attached to objects (Ono fig. 1: 102 discloses as a portable article) carried by the user (Ono ¶0033), a plurality of pieces of tag certification information (Ono ¶0033 discloses tag certification information as authentication information & ¶0036 discloses the authentication apparatus can receive authentication

information from a plurality of IC tags) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102) respectively (Ono fig. 3 & ¶0040 discloses the authentication holding unit holds the names of the articles for authentication and the authentication of the IC tags); a tag judgment unit (Ono integrated in the personal authentication unit; not shown but it's inherent) operable to judge whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition (Ono ¶0046-0047); and a permission unit (Ono fig. 2: 230 discloses as a processing unit) operable to permit a use of the function if the tag judgment unit (Ono not shown but it's inherent) judges that the level of match satisfies the predetermined condition (Ono ¶0038 discloses the process unit performs a desired process using the individual information of the IC card after the personal authentication unit has certified the right person), and each of the plurality of wireless IC tags (Ono fig. 1: 102a & ¶0036) comprising: a tag certification information storage unit (Ono not shown but it's inherent) operable to store a piece of tag certification information (Ono discloses as authentication information) for identifying a wireless IC tag (Ono fig. 1: 102a) storing the piece of tag certification information (Ono ¶0033 discloses the IC tag holds an authentication information, thus, the IC tag must have a storage unit. Ono fig. 3: 210 & ¶0040 discloses authentication information identifying an article, hence, a IC tag); and an output unit (Ono not shown but it's inherent) operable to output wirelessly the piece of tag certification information (Ono ¶0033 the IC tag outputs the authentication information by radio, thus, the device inherently has an output unit).

Ono does not disclose the authentication system comprising an identification information storage unit operable to store first identification information, and a user judgment unit operable to, if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, and the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user judgment unit judges that the first identification information matches the received second identification information.

Shinzaki discloses authentication system comprising an identification information storage unit (Shinzaki fig. 6: discloses as password information registration and storage unit) operable to store first identification information (Shinzaki discloses as password col. 12 lines 1-2), and a user judgment unit (Shinzaki fig. 6: password information matching check unit) operable to judge if the level of match does not satisfy the predetermined condition (Shinzaki fig. 7: S24 & col. 12 lines 36-40), receive second identification information (Shinzaki fig. 7: S30 discloses request user to input password) and judge whether or not the first identification information matches the received second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5). Once the authentication system authenticates the user at step S36, the user is allowed to use a function. Shinzaki fig. 7 further discloses that the system may authenticate the user by

receiving a password and determines if the password entered matches a stored password, hence, the authentication device permits use of the device by judging whether a stored optional authentication identification information matches an inputted authentication identification information.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono authentication system with the inclusion of Shinzaki password storage unit, as taught by Shinzaki. The combination of Ono in view of Shinzaki would yield to the claim limitation of "if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, wherein the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and if the user judgment unit judges that the first identification information matches the received second identification information".

The motivation would be to provide an additional feature to the user, for example, if the user did not have his/her wireless tag the user has the option to input a password to access the device.

2) In regard to claim 2, Ono discloses the claimed authentication apparatus (Ono fig. 1: 200) which permits a user to use a function provided by the authentication apparatus (Ono fig. 1: 200) if authenticity of the user is certified by authentication (Ono ¶0038 discloses the process unit (fig. 2: 210 which part of the authentication apparatus unit) performs a desired process after the user is authenticated), the authentication apparatus (Ono fig. 1: 200) comprising: a tag verification information storage unit (Ono fig. 2: 210 discloses as an Authentication Information Holding Unit) operable to store a plurality of pieces of tag verification information (Ono fig. 3: shows a plurality of tag verification information for each article stored in the authentication information holding unit) for identifying a plurality of wireless IC tags respectively (Ono ¶0036 & fig. 3 discloses that a plurality of articles can be received by the authentication apparatus); a receiving unit (Ono fig. 2: 230 & ¶0037 discloses the personal authentication unit serves also as an authentication information receiving unit) operable to wirelessly receive (Ono ¶0046, 0052 & 0057 discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from wireless IC tags (Ono fig. 1: 102a) attached to objects (Ono fig. 1: 102 discloses as a portable article) carried by the user (Ono ¶0033), a plurality of pieces of tag certification information (Ono ¶0046 discloses that the authentication information transmitted from the IC card and read by radio is identical with the authentication information selected from the authentication information holding unit, hence, it's obvious the IC card has a plurality of pieces of tag certification information) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102) respectively (Ono fig. 3 & ¶0040 discloses the

authentication holding unit holds the names of the articles for authentication and the authentication of the IC tags); a tag judgment unit (Ono integrated in the personal authentication unit; not shown but it's inherent) operable to judge whether or not a level of match between the plurality of pieces of tag verification information and the plurality of pieces of tag certification information satisfies a predetermined condition (Ono ¶0046-0047); and a permission unit (Ono fig. 2: 230 discloses as a processing unit) operable to permit a use of the function if the tag judgment unit (Ono not shown but it's inherent) judges that the level of match satisfies the predetermined condition (Ono ¶0038 discloses the process unit performs a desired process using the individual information of the IC card after the personal authentication unit has certified the right person).

Ono does not disclose the authentication apparatus comprising an identification information storage unit operable to store first identification information, and a user judgment unit operable to, if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information matches the received second identification information, and the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user judgment unit judges that the first identification information matches the received second identification information.

Shinzaki discloses authentication apparatus comprising an identification information storage unit (Shinzaki fig. 6: discloses as password information registration and storage unit) operable to store first identification information (Shinzaki discloses as password col. 12 lines 1-2), and a user judgment unit (Shinzaki fig. 6: password information matching check unit) operable to judge if the level of match does not satisfy the predetermined condition (Shinzaki fig. 7: S24 & col. 12 lines 36-40), receive second identification information (Shinzaki fig. 7: S30 discloses request user to input password) and judge whether or not the first identification information matches the received second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5). Once the authentication system authenticates the user at step S36, the user is allowed to use a function. Shinzaki fig. 7 further discloses that the system may authenticate the user by receiving a password and determines if the password entered matches a stored password, hence, the authentication device permits use of the device by judging whether a stored authentication optional identification information matches an inputted authentication identification information.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono authentication apparatus with the inclusion of Shinzaki password storage unit, as taught by Shinzaki. The combination of Ono in view of Shinzaki would yield to the claim limitation of "if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, receive second identification information and judge whether or not the first identification information

matches the received second identification information, wherein the permission unit permits the use of the function if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and if the user judgment unit judges that the first identification information matches the received second identification information".

The motivation would be to provide an additional feature to the user, for example, if the user did not have his/her wireless tag the user has the option to input a password to access the device.

3) In regard to claim 4 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 3, wherein

the first identification information is first biological information indicating biological characteristics of the user (Shinzaki col. 14 lines 22-39 discloses a fingerprint stored in the authentication device and used to authenticate a use if first biometric data is lower then a predetermined threshold),

the second identification information is second biological information indicating biological characteristics of the user (Shinzaki col. 14 lines 22-39 discloses a fingerprint data is inputted into the authentication device and used to authenticate the user if the user first biometric data is not higher then a predetermined threshold),

and if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user requests to be permitted to use the function, the

user judgment unit receives the second biological information and judges whether or not the first biological information and the received second biological information correspond to a same user (Shinzaki col. 14 lines 22-48 uses the second receive biometric data to authenticate a user (i.e., correspond that the receive data is the same user) , see fig. 9 for complete method).

4) In regard to claim 17 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 2, wherein each of the plurality of pieces of tag certification information contain a type code (Ono fig. 3: authentication information) indicating a type of an object to which a wireless IC tag identified by the piece of tag certification information is attached (Ono fig. 3 & ¶0046 discloses that the authentication information indicate the article the IC tag is attached to), and the tag judgment unit (Ono not shown but it's inherent) is further operable to judge whether or not a level of match between the plurality of pieces of tag verification information (Ono: authentication information) and one or more pieces of tag certification information (Ono ¶0046-0047), which remain after excluding, from the plurality of pieces of tag certification information received by the receiving unit (Ono fig. 2: 230), pieces of tag certification information that contain a predetermined type code, satisfies a predetermined condition (Ono ¶0044-0048 discloses the authentication apparatus uses weight coefficients of the tags to authenticate a user, hence, these weight coefficients are summed up and have to be greater than the reference value).

5) In regard to claim 19 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 2, wherein the tag judgment unit (Ono not shown but it's inherent) is further operable to judge whether or not a ratio of (i) a number of pieces of tag verification information that, among the plurality of pieces of tag verification information, match any of the plurality of pieces of tag certification information to (ii) a total number of the plurality of pieces of tag verification information stored in the tag verification information storage unit (Ono fig. 2: 210) is equal to or higher than a standard value (Ono fig. 6 & ¶0049-0053 discloses that the authentication system can authenticate the user by the IC card and the number of authentication articles, thus, it would be obvious at the time of the invention to authenticate a user by comparing the number of received authentication articles(IC tags) to the number of tags in the storage unit to a predetermined value).

6) In regard to claim 20 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 2, wherein the tag verification information storage unit (Ono fig. 2: 210) is further operable to store point values (Ono fig. 3: weight coefficients) indicating weights assigned to the plurality of pieces of tag verification information (Ono ¶0041), in correspondence with the plurality of pieces of tag verification information (Ono ¶0041 discloses that the weight correspond to the authentication information (tag verification information)), and the tag judgment unit (Ono not shown but it's inherent) is further operable to judge whether or not a ratio of (i) an acquired point value that is obtained by adding up point values corresponding to pieces

of tag verification information (Ono: authentication information) that, among the plurality of pieces of tag verification information (Ono: authentication information), match any of the plurality of pieces of tag certification information to (ii) a total point value that is obtained by adding up point values corresponding to the plurality of pieces of tag verification information (Ono: authentication information) stored in the tag verification information storage unit (Ono fig. 2: 210) is equal to or higher than a standard value (Ono 0052-0053 discloses that the weight coefficients (point value) are added up and compared to a reference value (total point value) and certifies the right person when the value is greater than the set reference number).

7) In regard to claim 21 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 2, wherein the tag verification information storage unit (Ono fig. 2: 210) is a portable recording medium (Ono fig. 9 & 0061 discloses that the IC card can integrate into the IC card the authentication information holding unit from fig. 2: 210, thus, it's inherent to swap the storage unit out of the authentication apparatus and place it in the IC card), and the portable recording medium is inserted in the authentication apparatus (Ono fig. 1: 100 discloses the IC card (portable recording medium) being inserted into the authentication apparatus).

8) In regard to claim 22, claim 22 the method claim is analyzed with respect to claim 1 the system claim.

9) In regard to claim 25 (dependent on claim 2), Ono in view of Shinzaki further discloses the authentication apparatus of claim 2, wherein

the first identification information is first character information being a combination of one or more numerals and/or one or more alphabets and/or one or more signs (col. 11, lines 21-26 discloses a password of number or digits is stored in the authentication device and used to authenticate the user if the authentication device does not authenticate the user at step S24 in fig. 7),

the second identification information is second character information being a combination of one or more numerals and/or one or more alphabets and/or one or more signs (col. 11, lines 21-26 discloses a password of number or digits is stored in the authentication device and the password is entered in order to authenticate a user), and

if the tag judgment unit judges that the level of match does not satisfy the predetermined condition, and the user requests to be permitted to use the function, the user judgment unit receives the second character information and judges whether or not the first character information matches the received second character information (fig. 7 and col. 12, lines 36-60).

5. Claims 5, 6, 8, 9, 11, 13, 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1) and further in view of Ogawa (PG-Pub No. 2005/0027990 A1).

1) In regard to claim 5 (dependent on claim 2), Ono and Shinzaki discloses the authentication apparatus of claim 2, wherein the plurality of pieces of tag verification information are a plurality of verification ID codes (Ono fig. 3: shows that the tag verification information are ID codes (i.e., authentication information & weight coefficients)) for identifying the plurality of wireless IC tags respectively (Ono fig. 3 shows the authentication information (i.e., 1125) stored in the authentication apparatus 200 authentication information holding unit 210 is used to identify the IC tags (i.e., 1125 identifies glasses)), the plurality of pieces of tag certification information are a plurality of certification ID codes (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, the certification ID codes is disclose as the authentication information & weight coefficients) for identifying the wireless IC tags (Ono fig. 1: 102a) attached to the objects respectively (Ono fig. 3 & ¶0041 it's obvious that the authentication information stored in the tag are codes (i.e., fig. 3: article 1125) that are used to identify the IC tags).

Ono and Shinzaki do not disclose that the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, acquire at least two certification ID codes out of the plurality of certification ID codes received by the receiving unit, and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes.

Ogawa discloses an authentication apparatus that comprises an update unit (Ogawa fig. 4: 405 discloses as an updating section) operable to, if a predetermined condition for update is satisfied (Ogawa ¶0080 & 0085 discloses generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string), acquire at least two codes (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string), and update contents of the storing section by storing (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section has the storing section store the transformation result and presentation symbol string) the at least two acquired codes into the storing section.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono and Shinzaki authentication apparatus with an update unit, as taught by Ogawa for the predictable result of updating the received codes for security reasons. The combination of Ono, Shinzaki and Ogawa would yield to the claim limitation "acquire at least two certification ID codes out of the plurality of certification ID codes received by the receiving unit, and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes".

The motivation would be to have an option to update a user authentication device tags associated with the user so the chances would decrease of someone impersonating the user of the device.

2) In regard to claim 6 (dependent on claim 5), Ono, Shinzaki and Ogawa further discloses the authentication apparatus of claim 5, wherein

the predetermined condition for update (Ogawa ¶0080 & 0085 discloses the predetermined condition as the generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string) is that the first identification information matches the second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5 & 46-50 discloses that the first identification information has to match the second identification, and Ogawa ¶0085 discloses that the update section causes the storing section to further store the presentation symbol when the transformation symbol string matches a transformation result), and

the update unit (Ogawa fig. 4: 405) updates the contents of the tag verification information storage unit if the first identification information matches the second identification information (Ogawa ¶0085 discloses that the update section causes the storing section (i.e., the tag verification information storage unit of Ono met in claim 1) to further store (i.e., update) the presentation symbol when the transformation symbol string matches a transformation result).

3) In regard to claim 8 (dependent on claim 5), Ono, Shinzaki and Ogawa further discloses the authentication apparatus of claim 5, wherein each of the plurality of certification ID codes (Ono fig. 3: authentication information & weight coefficients) contains a type code (Ono fig. 3: authentication information (e.g., 1125)) indicating a type of an object to which a wireless IC tag (Ono fig. 1: 102a) identified by the

certification ID code is attached (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, it's obvious the authentication information (certification ID codes) contain a type code (glasses) and the authentication information code (i.e.,) corresponds to that article (glasses see fig. 3)), and the update unit (Ogawa fig. 4: 405) is further operable to acquire at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes containing a predetermined type code (Ono fig. 3: authentication information column shows the predetermined type code for each article), from the plurality of certification ID codes received by the receiving unit (Ono fig. 2: 230).

4) In regard to claim 9 (dependent on claim 8), Ono, Shinzaki and Ogawa further disclose the authentication apparatus of claim 8, a priority level storage unit (Ono fig. 3 & ¶0048 Authentication Information Holding Unit Weight Coefficients Column discloses each article is given certain weights) operable to store a plurality of priority levels (Ono fig. 3: Weight Coefficients) with a plurality of type codes corresponding thereto (Ono fig. 3: shows the Authentication information corresponding to the Weight Coefficients), each of the plurality of priority levels indicating a recording priority with which a corresponding type code is recorded in an authentication recording medium for use in the judgment by the tag judgment unit (fig. 3: shows a weight coefficients (i.e., priority level) that has a

high priority and is at the top of the chart and corresponds to authentication information, thus, there is a sense of recording priority), wherein the predetermined type code is correlated with priority levels (Ono ¶0048) that are equal to or higher than a priority-level threshold value Ono fig. 4: Reference Value & ¶0048 discloses the reference value which is the value that all of the articles weight coefficients need to add up to in order for the user to be allowed the function of the authentication apparatus), and the update unit (Ogawa fig. 4: 405) is further operable to acquire at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes that have priority levels (Ono fig. 3: Weight Coefficient column) that are equal to or higher than the priority-level threshold value (Ono fig. 3 & 4 ¶0048 discloses the reference value which is the value that all of the articles weight coefficients need to add up to in order for the user to be allowed to use the function of the authentication apparatus), from the plurality of certification ID codes received by the receiving unit (Ono fig. 2: 230), and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority (Ogawa ¶0094-0096 discloses an authentication device whereby the updating unit receives two new codes and stores these values into the authentication device storage means corresponding to a user ID when a code is received by the receiving unit. At the same time, the sending unit transmits the new code(s) to the user device in order to update that the device with the new generated code. Thus, it would be obvious to

implement an update unit in the same fashion to Ono and Shinzaki authentication device for the predictable result of updating old codes with new codes).

5) In regard to claim 11 (dependent on claim 8), Ono, Shinzaki and Ogawa further disclose the authentication apparatus of claim 8,

a point storage unit (Ono fig. 3 & ¶0048 integrated into the authentication holding unit discloses as weight coefficient are summed up to authenticate a user) operable to store a plurality of point values (Ono fig. 3: weight coefficient column) with a plurality of type codes (Ono fig. 3: authentication information) corresponding thereto (Ono fig. 3: authentication information column corresponds to the weight coefficient column), wherein the predetermined type codes (Ono fig. 3: authentication information) are correlated with point values (Ono fig. 3: authentication information column corresponds to the weight coefficient column) that are equal to or higher than a point-value threshold value (Shinzaki col. 12 lines 51-60 discloses that the password and biometrics of a user has to be equal to or larger than the threshold and then the user is authenticated), and the update unit (Ogawa fig. 4: 405) is further operable to acquire at least two (Ogawa fig. 4: 405 & 403 & 0094 discloses the updating section receives the transformation result and presentation symbol string) certification ID codes (Ono fig. 3: authentication information & weight coefficients) that have point values (Ono fig. 3: weight coefficient column) that are equal to or higher than the point-value threshold value (Shinzaki col. 12 lines 51-60 discloses that the password and biometrics of a user has to be equal to or larger than the threshold and then the user is authenticated), from the plurality of

certification ID codes received by the receiving unit (Ono ¶0036), and update contents of the tag verification information storage unit by storing the at least two acquired certification ID codes into the tag verification information storage unit as verification ID codes by priority (Ogawa ¶0085 discloses that the update section causes the storing section to further store (i.e., update) the presentation symbol (i.e., authentication information and weight coefficients of Ono) when the transformation symbol string matches a transformation result).

6) In regard to claim 13 (dependent on claim 2), Ono and Shinzaki further disclose the authentication apparatus of claim 2, wherein the plurality of pieces of tag verification information are a plurality of pieces of unique authentication data for verification (Ono fig. 3 shows in the authentication holding unit 210 a plurality of unique authentication data (authentication information and weight coefficients)) assigned by the authentication apparatus (Ono ¶0040), the plurality of pieces of tag certification information are a plurality of pieces of unique authentication data for certification assigned by the authentication apparatus (Ono ¶0046 discloses that the authentication information read by radio is identical with the authentication information selected from the authentication information holding unit (see fig. 3 for the information contained in the authentication information holding unit), thus, the plurality of pieces of unique authentication data is disclosed as the authentication information & weight coefficients), the receiving unit (Ono fig. 2: 230) wirelessly receives (Ono ¶0046, 0052 & 0057

discloses the personal authentication unit reads out the authentication information by radio from the IC tags), from the wireless IC tags (Ono fig. 1: 102a) attached to the objects (Ono fig. 1: 102 discloses as a portable article), a plurality of ID codes for identifying the wireless IC tags attached to the objects respectively (Ono ¶0036). Ono further discloses that the device comprises a transmission unit (Ono not shown but it's inherent) operable to transmit a signal to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification (Ono ¶0046 discloses that the authentication apparatus transmits a signal to the IC tags corresponding to the article it is associated with).

Ono and Shinzaki do not disclose the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, generate a different piece of authentication data for each ID code received by the receiving unit, acquire at least two pieces of authentication data from pieces of generated authentication data, and update contents of the tag verification information storage unit by storing the at least two pieces of acquired authentication data into the tag verification information storage unit as authentication data for verification, and a transmission unit operable to transmit, for each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a piece of authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification.

Ogawa discloses authentication apparatus that updates all the devices in the system with all new codes comprising an update unit (Ogawa fig. 4: 405 discloses as an

updating section) operable to, if a predetermined condition for update is satisfied (Ogawa ¶0080 & 0085 discloses generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string) acquire at least two pieces of data of generated data (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string), and update contents of the storage section by storing the at least two pieces of acquired data into the storage section to be use for authentication (Ogawa fig. 4: 405 & 403 & ¶0094-0096 discloses the updating section has the storing section store the transformation result and presentation symbol string).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono and Shinzaki authentication apparatus to include an update unit in order update coded information for the device, as taught by Ogawa. The combination of Ono, Shinzaki and Ogawa would yield to the claim limitation " the authentication apparatus further comprises an update unit operable to, if a predetermined condition for update is satisfied, generate a different piece of authentication data for each ID code received by the receiving unit, acquire at least two pieces of authentication data from pieces of generated authentication data, and update contents of the tag verification information storage unit by storing the at least two pieces of acquired authentication data into the tag verification information storage unit as authentication data for verification, and a transmission unit operable to transmit, for each piece of authentication data for verification having been updated by the update unit, a piece of authentication data for verification as a piece of authentication data for

certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification".

The motivation would be to provide an addition security feature to a user, for example, there is a high possibility that data may be stolen when transmitted wirelessly this would improve and insure a safe authentication by the device (Ogawa ¶0007-0009).

7) In regard to claim 14 (dependent on claim 13), Ono, Shinzaki and Ogawa further disclose the authentication apparatus of claim 13,

wherein the predetermined condition for update (Ogawa ¶0080 & 0085 discloses the predetermined condition as the generating section 420 generates a symbol string which is the condition needed for the updating section to store the presentation string) is that the first identification information matches the second identification information (Shinzaki fig. 7: S33 & col. 12 lines 2-5 & 46-50 discloses that the first identification information has to match the second identification, and Ogawa ¶0085 discloses that the update section causes the storing section to further store the presentation symbol when the transformation symbol string matches a transformation result), and

if the first identification information matches the second identification information, the update unit updates the contents of the tag verification information storage unit (Ogawa ¶0085 discloses that the update section causes the storing section to further store the presentation symbol when the transformation symbol string matches a transformation result), and the transmission unit transmits (Ono not shown but it's inherent), for each piece of authentication data for verification having been updated by

the update unit (Ogawa ¶0085 discloses the update section stores a new code in the storing section), a piece of authentication data for verification as a piece of authentication data for certification, to a wireless IC tag having an ID code corresponding to the piece of authentication data for verification (Ogawa fig. 3 and ¶0085 discloses that the sending section sends all the codes need to the user device in order for the user to be authenticated in the future).

8) In regard to claim 16 (dependent on claim 13), Ono, Shinzaki and Ogawa further disclose the authentication apparatus of Claim 13, wherein each of the plurality of ID codes contains a type code (Ono fig. 3: discloses as authentication information) indicating a type of an object to which a wireless IC tag identified by the ID code is attached (Ono fig. 1: 102a & fig. 3 shows that the tag attached to the glasses has a code in the authentication table that is associated with the article column). Ono in view of Ogawa combination would yield to the claim limitation "the update unit is further operable to acquire at least two pieces of authentication data corresponding to ID codes that include a predetermined type code among the plurality of ID codes received by the receiving unit (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string)".

6. Claims 7 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1) and in

view of Ogawa (PG-Pub No. 2005/0027990 A1) and further in view of Arens (PG-Pub No. 2001/0030603 A1).

1) In regard to claim 7 (dependent on claim 5), Ono in view of Ogawa discloses the authentication apparatus of claim 5.

Ono in view Ogawa does not disclose the authentication apparatus comprising a distance calculating unit operable to measure values of a response time during communication between the authentication apparatus and each of the wireless IC tags attached to the objects, and calculate values of a distance between the authentication apparatus and each of the wireless IC tags attached to the objects based on the measured values of the response time, wherein the update unit is further operable to acquire at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes.

However, it is well known in the art of location systems that a first device can be determined to exceed a predetermined distance from a second device by measuring the response time of the signals transmitted and determining the distance between the two devices. Arens discloses a location system comprising a distance calculating unit (fig. 7: 70 discloses as a timer) operable to measure values of a response time during communication between the device 2 and device 1 (¶0038), and calculate values of a distance between device 2 and device 1 based on the measured values of the response time (¶0039 discloses the distance is determined (i.e., calculated) by the time recorded by the timer). Arens further discloses that the calculated values of the distance are

compared to a predetermined value to see if the two devices are separated by more than the predetermined value (fig. 2: 26 and ¶0024).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view Ogawa authentication apparatus to include a distance calculating unit, as taught by Arens for the predictable result of alerting a user when he/she is out of the range of a device in which authenticates the user. The combination of Ono, Shinzaki, Ogawa and Ares would yield to the claim limitation "a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of certification ID codes have been received, wherein the update unit is further operable to acquire at least two certification ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, from the plurality of received certification ID codes (Hence, with the addition of Ares distance calculating unit, Ono in view of Shinzaki and Ogawa authentication apparatus would obviously be motivated to validate the codes that are determined to be within a certain range which would be done by the update unit, since these are the only codes that the device can be certain are in the proximity of the device)".

The motivation would be to provide an additional feature to the device in which would allow the system to become more secure. For example, if a user leaves the proximity without logging off the authentication device the distance calculating means may insure that the device is shut down and no one can come behind the user and use the device without his/her knowledge.

2) In regard to claim 15 (dependent on claim 13), Ono in view of Shinzaki and Ogawa discloses the authentication apparatus of claim 13 wherein the update unit (Ogawa fig. 4: 405) acquires at least two pieces of data corresponding to ID codes among the received ID codes (Ogawa ¶0094 discloses updating section receives a transformation result and presentation symbol string).

Ono in view of Ogawa does not disclose the authentication apparatus further comprising a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of ID codes have been received, wherein the update unit acquires at least two pieces of authentication data corresponding to ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, among the plurality of received ID codes.

However, it is well known in the art of location systems that a first device can be determined to exceed a predetermined distance from a second device by measuring the response time of the signals transmitted and determining the distance between the two devices. Arens discloses a location system comprising a distance calculating unit (fig. 7: 70 discloses as a timer) operable to measure values of a response time during communication between the device 2 and device 1 (¶0038), and calculate values of a distance between device 2 and device 1 based on the measured values of the response time (¶0039 discloses the distance is determined (i.e., calculated) by the time recorded by the timer). Arens further discloses that the calculated values of the distance are

compared to a predetermined value to see if the two devices are separated by more than the predetermined value (fig. 2: 26 and ¶0024).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono in view of Shinzaki and Ogawa authentication apparatus to provide a feature to determine the distance between the authentication apparatus and IC tag, as taught by Ares. The combination of Ono in view of Shinzaki, Ogawa and Ares would yield to the claim limitation "the authentication apparatus further comprising a distance calculating unit operable to calculate values of a distance between the authentication apparatus and each of the wireless IC tags from which the plurality of ID codes have been received, wherein the update unit acquires at least two pieces of authentication data corresponding to ID codes for which calculated values of the distance are each equal to or lower than a predetermined value, among the plurality of received ID codes (Hence, with the addition of Ares distance calculating unit, Ono in view of Shinzaki and Ogawa authentication apparatus would obviously be motivated to validate the codes that are determined to be within a certain range which would be done by the update unit, since these are the only codes that the device can be certain are in the proximity of the device)".

The motivation would be to provide an additional feature of authentication of a user without imposing a burden on the user of the device.

7. Claims 10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1)

in view of Ogawa (PG-Pub No. 2005/0027990 A1) and further in view of Omae (PG-Pub No. 2006/0174121 A1).

1) In regard to claim 10 (dependent on claim 9), Ono, Shinzaki and Ogawa discloses the authentication apparatus of claim 9.

Ono, Shinzaki and Ogawa does not disclose the authentication apparatus comprising a priority level update unit operable to receive a type code and a priority level, and update the priority level storage unit by replacing a priority level, which is stored in the priority level storage unit in correspondence with the received type code, with the received priority level.

Omae discloses security system that comprises a priority level update unit operable to receive (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) and update external devices by replacing a priority level (Omae fig. 8: 2 & 3 & ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the priority level of a device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono, Shinzaki and Ogawa authentication apparatus to include a priority level update unit, as taught by Omae. The combination of Ono, Shinzaki and Ogawa and Omae would yield to the claim limitation "a priority level update unit operable to receive a type code, and update the priority level storage unit by replacing a priority level, which is stored in the priority level storage unit in correspondence with the received type code, with the received priority level".

The motivation would be to simplify management process of the group management server without reducing the security (Omae ¶0017).

2) In regard to claim 12 (dependent on claim 11), Ono, Shinzaki and Ogawa discloses the authentication apparatus of Claim 11.

Ono, Shinzaki and Ogawa does not disclose the authentication apparatus comprises a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in the point storage unit in correspondence with the received type code, with the received point value.

Omae discloses an apparatus that comprises an update unit operable to receive a code (Omae fig. 8: discloses as Device ID/Attribute Setting and Update Unit that is operable to receive a device ID, ¶0069) and update a value (Omae ¶0069 discloses that the Device ID/Attribute Setting and Update Unit can change the value of a device). Although Omae may not disclose his device is used as a point update unit, it would have been obvious to replace Omae update unit in order to update a value of a device, there by increasing the security of the authentication device.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono, Shinzaki and Ogawa authentication apparatus with a update unit to bring up to date the values stored in the device, as taught by Omae. The combination of Ono, Shinzaki and Ogawa and Omae would yield to the claim

limitation "a point update unit operable to receive a type code and a point value, and update the point storage unit by replacing a point value, which is stored in the point storage unit in correspondence with the received type code, with the received point value".

The motivation would be to simplify management process of the group management server without reducing the security (Omae ¶0017).

8. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1) and further in view of Zhang (PG-Pub. No. 2004/0064698 A1).

1) In regard to claim 18 (dependent on claim 2), Ono and Shinzaki discloses the authentication apparatus of claim 2 further comprising a control unit (Ono fig. 2: 230 & ¶0037 discloses as a personal authentication unit) operable to control the receiving unit (Ono fig. 2: 230) to receive the plurality of pieces of tag certification information (Ono ¶0046 discloses the personal authentication system is the element that reads controls the transmit signal that is sent to the IC tags).

Ono and Shinzaki do not disclose the authentication apparatus of claim 2, wherein the tag verification information storage unit further stores expiration date/time information that indicates an expiration date/time of each piece of tag verification information, and the authentication apparatus further comprises a control unit operable to, if having judged that any expiration date/time of the plurality of pieces of tag

verification information has not been reached, control the receiving unit to receive the plurality of pieces of tag certification information.

Zhang discloses an authentication system that stores expiration date/time information that indicates an expiration date/time of access to the device (Zhang ¶0223 discloses that the apparatus can store a date or time of expiration in which a user has access to a device).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ono and Shinzaki authentication apparatus to associate an expiration time or date with information received by the authentication apparatus, as taught by Zhang. The combination of Ono in view of Shinzaki and Zhang would yield to the claim limitation "the tag verification information storage unit further stores expiration date/time information that indicates an expiration date/time of each piece of tag verification information, and the authentication apparatus further comprises a control unit operable to, if having judged that any expiration date/time of the plurality of pieces of tag verification information has not been reached, control the receiving unit to receive the plurality of pieces of tag certification information".

The motivation would be to provide the user with an additional feature, for example, by associating expiration date or time with the information transmitted to the device this would increase the security level for the user.

9. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ono (PG-Pub. No. 2004/0139020 A1) in view of Shinzaki (Pat. No. 7,007,298 B1).

1) In regard to claim 24, claim 24 is directed toward embody the method of claim 22 in a "computer readable medium".

Ono does not disclose a computer-readable recording medium recording therein an authentication program that causes a computer to operate as an authentication apparatus which permits a user to use a function provided by the authentication apparatus if authenticity of the user is certified by authentication.

It would have been obvious to embody the procedures of Ono discussed with respect to claim 22 in a "computer readable medium" in order that the instructions could be automatically performed by a processor.

Response to Arguments

10. Applicant's arguments with regard to claims 1, 2, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 and 22, filed on the 20 November 2009 have been fully considered but they are not persuasive.

1) As to claims 1, 2 and 24, on pages 16-18 and 24 of Applicant's Response, applicant argues that modifying Ono with Shinzaki to achieve the user judgment unit and permission unit as recited in claim 1 would render Ono unsatisfactory for its intended purpose. Specifically Applicant argues, on page 17, "by modifying Ono with the password feature of Shinzaki, the combination would render the modified Ono reference unsatisfactory for its intended purpose, i.e., by modifying Ono to authenticate a user with a password, it defeats Ono's intended purpose of not using a password in authentication."

The Examiner recognizes that the Ono reference did disclose that requiring a person to remember a password in the context of using recorded data in a tag for authentication poses a burden on the user ([0006]). However, the Examiner respectfully disagrees with Applicant's arguments that the inclusion of a password defeats Ono's intended purpose, because the placing of recorded data in a tag does not necessarily disallow/prevent the use of a password in Ono. This is evident by the use of a personal ID for input into a terminal that will authenticate the user in fig. 10 that is also taught by Ono. Hence, the user would still have to memorize the personal ID in order for the terminal to authenticate the user. Furthermore, the user of the system/apparatus does not have to burden him/her self with memorization of the password. The user can always write/store in a safe place the password he/she needs to log in/out of a terminal. Finally, the secondary reference discloses a password as a secondary option used only to authenticate the user if the first authentication data is lower then a predetermined threshold.

Therefore, Applicant's arguments art not deemed persuasive to overcome the rejections. Applicant's arguments with regard to claims 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 and 22 that are dependent on claim 1 or 2 arguments are therefore not persuasive.

2) As to claims 4 and 25, on pages 19 and 25-26 of Applicant's Response respectfully, applicant argues that the Examiner has not sufficiently demonstrated that the above combination of Ono and Shinzaki renders claim 4 *prima facie* obvious.

Specifically Applicant argues, on page 18-19, "by modifying Ono with the password feature of Shinzaki, the combination would change the principle operation of the Ono reference unsatisfactory, i.e., by modifying Ono to authenticate a user with a password, it defeats Ono's intended purpose of not using a password in authentication"

The Examiner recognizes that the Ono tries to reduce the need of a password by using recorded data in a tag for convenience. However, the Examiner respectfully disagrees with Applicant's arguments that the inclusion of a password defeats Ono's intended purpose because the placing of recorded data in a tag does not necessarily disallow/prevent the use of a password. This is evident by the use of a personal ID for input into a terminal that will authenticate the user in fig. 10. Hence, the user would still have to memorize the personal ID in order for the terminal to authenticate the user. Furthermore, the user of the system/apparatus does not have to burden him/her self with memorization of the password. The user can always write/store in a safe place the password he/she needs to log in/out of a terminal. Finally, the secondary reference discloses a password is a way to supplement a non-password authentication means with the alternative or back-up password.

Therefore, Applicant's arguments art not deemed persuasive to overcome the rejections. See above rejection for more details for amended claim 9 and newly added claim 25 rejection.

3) As to claim 9, on pages 20-21 of Applicant's Response, applicant argues that neither Ono, Shinzaki nor Ogawa discloses or suggest the priority storage unit as

recited in claim 9. Specifically Applicant argues, on page 21, "the weight coefficients correspond to a probability a user is carrying the object having the IC tag."

The Examiner respectfully disagrees with Applicant's arguments because the probability is the reason why Ono chose the particular weight coefficients/priority for the corresponding article. This is no different from what is explained in figure 4 of Applicant's disclosure.

Therefore, Applicant's arguments art not deemed persuasive to overcome the rejections. See above rejection for more details. Applicant argument with regard to claim 10 dependent on claim 9 arguments is therefore not persuasive.

4) Applicant's arguments with respect to claims 7 and 15 have been considered but are moot in view of the new ground(s) of rejection necessitated by amendment to the claims.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1) Simonen (PG-Pub. No. 2006/0036855 A1)

-- Similar inventive concept

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Curtis J. King whose telephone number is (571)270-5160. The examiner can normally be reached on Mon-Thurs 7:30 - 6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Benjamin C. Lee can be reached on (571)272-2963. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ck/

/BENJAMIN C. LEE/
Supervisory Patent Examiner, Art Unit 2612